

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for resolving an addressing conflict between a first processor in a first network and a second processor in a second network, the method comprising:

detecting the addressing conflict between a first address of the first processor and a second address of the second processor, prior to receiving packets from the processors;

associating ~~an identifier~~a tunnel ID with the detected addressing conflict; receiving from the first processor one or more packets forming a tunnel; removing from the one or more packets information about the tunnel, the removed tunnel information including a virtual address of the tunnel;

determining that the one or more packets are associated with the detected addressing conflict by determining that the removed virtual address corresponds to the ~~identifier~~tunnel ID associated with the detected addressing conflict;

determining a translated address based on the removed virtual address; and forwarding the one or more packets based on the translated address.

2. (Previously Presented) The method of claim 1, wherein said step of detecting further comprises the step of:

detecting that the first address is the same as the second address.

3. (Previously Presented) The method of claim 1, wherein said step of detecting further comprises the step of:

detecting that the first address is the same as the second address based on information about the first processor and the tunnel.

4. (Previously Presented) The method of claim 1, wherein said step of removing further comprises the step of:

removing information indicating the virtual address, the virtual address uniquely identifying the tunnel.

5. (Previously Presented) The method of claim 1, wherein said step of removing further comprises the step of:

removing information indicating a virtual IP address of the tunnel.

6. (Currently Amended) The method of claim 1, wherein said step of determining that the one or more packets are associated with the detected addressing conflict further comprises the step of:

determining, based on the removed virtual address and the ~~identifier~~ tunnel ID, that the first address in the one or more packets causes the addressing conflict.

7. (Original) The method of claim 1, wherein said step of determining the translated address further comprises the step of:

determining the translated address based on the first address.

8. (Original) The method of claim 1, wherein said step of determining the translated address further comprises the step of:

mapping the first address into the translated address, such that the one or more packets are forwarded on a network other than the first and second networks without the addressing conflict.

9. (Original) The method of claim 1, wherein said step of determining the translated address further comprises the step of:

mapping the first address into the translated address, such that the one or more packets are forwarded on the second network without the addressing conflict.

10. (Original) The method of claim 1, wherein said step of determining the translated address further comprises the step of:

mapping the first address into the translated address, such that the one or more packets are forwarded on the first network without the addressing conflict.

11. (Original) The method of claim 10, further comprising the step of:
mapping, at a gateway, the first address into the translated address.

12. (Original) The method of claim 1, wherein said step of detecting further comprises the step of:

detecting the addressing conflict at a gateway interfacing a network other than the first and second networks.

13. (Original) The method of claim 1, wherein said step of detecting further comprises the step of:

detecting the addressing conflict at a gateway interfacing the second network.

14. (Original) The method of claim 1, wherein said step of detecting further comprises the step of:

detecting the addressing conflict at a gateway interfacing the first network.

15. (Currently Amended) An apparatus comprising:

a memory including code that detects an addressing conflict between a first address of a first processor in a first network and a second address of a second processor in a second network prior to receiving packets from the processors, associates ~~an identifier-a tunnel ID~~ with the detected addressing conflict, receives from the first processor one or more packets forming a tunnel, removes from the one or more packets a virtual address of the tunnel, determines that the one or more packets are associated with the detected addressing conflict by determining that the removed virtual address corresponds to the ~~identifier~~tunnel ID associated with the detected addressing conflict, determines a translated address based on the removed virtual address, and forwards the one or more packets based on the translated address; and at least one processor that executes the code.

16. (Previously Presented) The apparatus of claim 15, wherein said code detects that the first address is the same as the second address.
17. (Previously Presented) The apparatus of claim 15, wherein said code detects that the first address is the same as the second address based on information about the first processor and the tunnel.
18. (Previously Presented) The apparatus of claim 15, wherein said code removes the virtual address, the virtual address uniquely identifying the tunnel.
19. (Previously Presented) The apparatus of claim 15, wherein said code removes information including a virtual IP address of the tunnel.
20. (Previously Presented) The apparatus of claim 15, wherein said code determines, based on the removed virtual address, that the first address in the one or more packets causes the addressing conflict.
21. (Original) The apparatus of claim 15, wherein said code determines the translated address based on the first address.

22. (Original) The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded on a network other than the first and second networks without the addressing conflict.

23. (Original) The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded to the second network without the addressing conflict.

24. (Original) The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded to the first network without the addressing conflict.

25. (Original) The apparatus of claim 15, further comprising:
code that maps, at a gateway, the first address into the translated address.

26. (Currently Amended) A computer-implemented system, comprising:
means for detecting an addressing conflict between a first address of a first processor on a first network and a second address of a second processor on a second network, prior to receiving packets from the processors;

means for associating ~~an identifier~~ a tunnel ID with the detected addressing conflict;

means for receiving from the first processor one or more packets forming a tunnel;

means for removing from the one or more packets information about the tunnel,
the removed tunnel information including a virtual address of the tunnel;

means for determining that the one or more packets are associated with the
detected addressing conflict by determining that the removed virtual address
corresponds to the identifier-tunnel ID associated with the detected addressing conflict;

means for determining a translated address based on the removed virtual
address; and

means for forwarding the one or more packets based on the translated address.

27. (Previously Presented) The system of claim 26, wherein said means for
detecting detects that the first address is the same as the second address.

28. (Previously Presented) The system of claim 26, wherein said means for
detecting detects that the first address is the same as the second address based on
information about the first processor and the tunnel.

29. (Previously Presented) The system of claim 26, wherein said means for
removing removes from the one or more packets the virtual address, the virtual address
uniquely identifying the tunnel.

30. (Previously Presented) The system of claim 26, wherein said means for
removing removes from the one or more packets information indicating a virtual IP
address of the tunnel.

31. (Previously Presented) A network, comprising:
a first processor having a first address on a first network;
a second processor having a second address on a second network; and
a processor other than the first and second processors that detects a conflict
between the first address and the second address prior to communication between the
first processor and the second network and resolves the conflict based on address
translation information retrieved using a virtual address of a tunnel established between
the other processor and the first network, such that communication between the first
processor and the second network is enabled.

32. (Previously Presented) The network of claim 31, wherein the other
processor determines a translated address based on the virtual address of the tunnel
and forwards one or more packets to the second network based on the translated
address.

33. (Original) The network of claim 31, wherein the other processor functions
as a gateway.

34. (Previously Presented) The network of claim 31, wherein the other
processor resolves the conflict based on another virtual address of another tunnel
established between the other processor and the second network.

35. (Original) The network of claim 31, wherein the other processor resolves the conflict such that communication between the second processor and first network is enabled.

36. (Previously Presented) The method of claim 1, further comprising the step of:

forming the tunnel, such that a first protocol encapsulates a second protocol.

37. (Previously Presented) The method of claim 36, further comprising the step of:

using the first protocol as an Internet Protocol (IP).

38. (Previously Presented) The method of claim 36, further comprising the step of:

using the second protocol as an Internet Protocol (IP).

39. (Previously Presented) The method of claim 38, further comprising the step of:

defining the second protocol to further include an encryption protocol.

40. (Previously Presented) The method of claim 1, further comprising the step of:

removing from the one or more packets the virtual address of the tunnel, the virtual address uniquely identifying the tunnel and being routable on a virtual network.

41. (Previously Presented) The method of claim 1, wherein said determining the translated address further comprises the step of:

determining the translated address, such that the addressing conflict is resolved with respect to the first network without regard to a possible addressing conflict on a network other than the first network.

42. (Previously Presented) The method of claim 1, wherein said determining the translated address further comprises the step of:

determining the translated address, such that the addressing conflict is resolved between the first and second networks without regard to a possible addressing conflict on a network other than the first and second networks.

43. (Previously Presented) The method of claim 1, wherein said determining the translated address further comprises the step of:

determining the translated address, such that the addressing conflict is resolved without consent of another processor.

44. (Canceled)

45. (Previously Presented) The apparatus of claim 15, further comprising:
code that forms the tunnel, such that a first protocol encapsulates a second
protocol.

46. (Previously Presented) The apparatus of claim 45, further comprising:
code that uses the first protocol as an Internet Protocol (IP).

47. (Previously Presented) The apparatus of claim 45, further comprising:
code that uses the second protocol as an Internet Protocol (IP).

48. (Previously Presented) The apparatus of claim 47, further comprising:
code that uses the second protocol to further include an encryption protocol.

49. (Previously Presented) The apparatus of claim 15, further comprising:
code that removes from the one or more packets the virtual address of the
tunnel, the virtual address being routable on a virtual network.

50. (Previously Presented) The apparatus of claim 15, wherein said code that
determines the translated address further comprises:
code that determines the translated address, such that the addressing conflict is
resolved with respect to the first network without regard to a possible addressing conflict
on a network other than the first network.

51. (Previously Presented) The apparatus of claim 15, wherein said code that determines the translated address further comprises:

code that determines the translated address, such that the addressing conflict is resolved between the first and second networks without regard to possible addressing conflicts on a network other than the first and second networks.

52. (Previously Presented) The apparatus of claim 15, wherein said code that determines the translated address further comprises:

code that determines the translated address, such that the addressing conflict is resolved without consent of a first gateway coupled to the first network.

53. (Previously Presented) The apparatus of claim 52, wherein said code that determines the translated address further comprises:

code that determines the translated address, such that the addressing conflict is resolved without consent of a second gateway coupled to the second network.

54. (Previously Presented) The network of claim 31, wherein the other processor determines the translated address without regard to the first and second networks, such that the addressing conflict is resolved locally on a network other than the first and second networks.

55. (Previously Presented) The network of claim 31, wherein the other processor determines the translated address, such that the addressing conflict is resolved on a network other than the first and second networks.

56. (Currently Amended) The method of claim 1, further comprising storing the translated address with the ~~identifier~~ tunnel ID associated with the detected addressing conflict; and

wherein determining a translated address based on the removed virtual address comprises retrieving, based on the ~~identifier~~ tunnel ID, information indicating the translated address.